Doc. No. 78-4039-03

Cisco Micro Webserver Version 1.2 Release Notes

April 28, 1997

The *Cisco Micro Webserver Version 1.2 Release Notes* describe system considerations and caveats for Cisco Micro Webserver version 1.2 and include instructions on how to upgrade your system.

Note The Micro Webserver product includes ZIP disk software, software utilities, and firmware. Currently, the ZIP software and utilities are at version 1.1. The firmware is at version 1.2.

The Cisco Micro Webserver is a versatile Web server appliance that is easy to install and cost-effective. It can be used for entry-level World Wide Web hosting, to set up a corporate workgroup intranet, as a network documentation server, or Trivial File Transfer Protocol (TFTP) and Syslog server, or as an offline kiosk. See also http://www.cisco.com/microweb or refer to your *Cisco Micro Webserver Quick Reference Guide* and *Using Cisco Micro Webserver* guide.

These release notes discuss the following topics:

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Platform Support

Table 1 provides a matrix of Cisco Micro Webserver applications support per platform.

Table 1 Cisco Micro Webserver Applications Support Per Platform

Feature	Windows 95/ Windows NT 4.x	Windows 3.1	UNIX	Macintosh
Java applets[1]	yes	yes	yes	yes
BOOTP Server application	yes	no	no	no
File Transfer Utility	yes	no	no	no
Form Builder application	yes	no	no	no

[1] Requires Java-enabled browser.

Upgrading Your Micro Webserver

This section describes how to upgrade your Micro Webserver from an earlier version.

Note While Micro Webserver firmware is at version 1.2, ZIP disk software and software utilities are at version 1.1.

For a successful upgrade, you'll need to complete these steps in order:

1. Get a copy of the latest firmware, software, and utilities.
2. Upgrade your Micro Webserver ZIP disk contents.
3. Upgrade your Micro Webserver firmware.
4. Upgrade the software utilities (BOOTP Server, File Transfer Utility, and Form Builder).

   Software utilities are supported only on Windows 95 and Windows NT 4.x platforms.

Upgrade procedures are described in detail in the following sections.

Note Cisco recommends that you have a minimum of 16 MB RAM on your workstation to accommodate the upgrade process. The ZIP files and their extracted directories will require approximately 17 MB of disk space.

Getting a Copy of Firmware, Software, and Utilities

You can obtain a Micro Webserver files at the Cisco Connection Online (CCO) Web site. To download the software from CCO, you must have an account. If you do not have an account, see your customer service representative for more information.

Step 1 Go to http://www.cisco.com/kobayashi/sw-center/index.shtml. Then find the Cisco Micro Webserver section under Internet Products.

Step 2 Download the following ZIP files to a temporary directory your local hard drive (for example, c:/upgrade):

- mweb_readme12.txt (upgrade procedure notes)
- mweb_fware12.ZIP (firmware upgrade file)
- mweb_util11.ZIP (software utilities upgrade file)
- mweb_zip11.ZIP (zip disk upgrade file)

Upgrading the ZIP Disk

To upgrade to Micro Webserver ZIP disk software version 1.1:

Step 1 Unzip the mweb_zip11.ZIP file to a temporary directory on your local hard drive. For example, unzip the file contents to c:/upgrade/zipdisk.

Note For Windows platforms, Cisco recommends the use of WinZip to unzip the Cisco compressed files.

After the file is unzipped, you will see these directories: /cisco, /etc, /forms, quick_ref_card, and mweb_readme12.txt.

Step 2 Open a file transfer program. For example, use the Micro Webserver File Transfer Utility or FTP.

Step 3 Use the file transfer program to connect to your Micro Webserver and log in as “root.”

Step 4 As a backup precaution, rename the /zip-100/cisco directory on your Micro Webserver to /zip-100/cisco_old.

Step 5 Of the unzipped directories you now have, copy *only* the /cisco directory from your local hard drive to the /zip-100 directory on your Micro Webserver.

Caution Do *not* copy any of the other unzipped directories (/etc, /forms, quick_ref_card, and mweb_readme12.txt) to your Micro Webserver. You may overwrite important data files you have created with version 1.0.

Step 6 To verify the upgrade, go to http://<*webserver hostname*/configure>.

You should see version 1.1 at the top of the Login tab. If you do not see version 1.1, clear the disk and memory caches on your Web browser and try again. If this action does not refresh the Micro Webserver version, quit and relaunch your Web browser. Then try http://<*webserver hostname*/configure> again.

Step 7 After a successful copy, delete the /zip-100/cisco_old directory from your Micro Webserver.

Upgrading the Firmware

This section provides two separate procedures for upgrading to firmware version 1.2:

- *If you are using a Windows or Unix platform*, read only the first section, “Windows and UNIX Platforms”.
- *If you are using a Macintosh system,* skip to “Macintosh Platforms,” page 5.

Windows and UNIX Platforms

To upgrade your Micro Webserver firmware:

Step 1 Unzip the mweb_fware12.ZIP file to a temporary directory on your local hard drive. For example, unzip the file contents to c:/upgrade/fware.

Note For Windows platforms, Cisco recommends the use of WinZip to unzip the Cisco compressed files.

After the file is unzipped, you will see the Mw_r1024.hex file.

Step 2 Open a file transfer program.

For example, use the Micro Webserver File Transfer Utility or FTP.

Step 3 Copy the Mw_r1024.hex file from your local hard drive to the /zip-100 directory on your Micro Webserver.

Step 4 Using your Web browser, go to http://<*webserver hostname*>/configure.

Step 5 Log in to your Micro Webserver as root.

Step 6 Your Micro Webserver document root must be set to /. If the document root is set to another path, the system cannot locate the firmware file.

To change the document root setting to /, select the **Basic** tab and enter / in the Document Root field. Then click **Apply** and click **Save**.

Step 7 Select the **Upgrade** tab.

Step 8 In the Firmware Location field, enter the filename with the complete path of the file containing the latest firmware. You can also use the Browse button function to locate this file.

Step 9 Enter the root password (if it has been set) in the Reenter Password field.

Step 10 Click **Upgrade**.

The firmware in the source file will load to NVRAM in the Micro Webserver. The process will take a few minutes. The percentage (%) bar and status message (lower lefthand corner of window) will indicate progress.

Note When the “Firmware upgrade successful message” appears, continue to wait until the Micro Webserver reboots (it takes no more than 90 seconds). During this interval, the server is updating its Flash memory. While rebooting, the LED on the front of the Micro Webserver flashes red and green, and the 100% indication in the percentage bar flashes. Do *not* power off the Micro Webserver at this time. When the reboot is complete, the LED provides a blinking green indication and the 100% indication in the percentage bar stops flashing.

Step 11 To verify the firmware upgrade, Telnet to your Micro Webserver and check the login banner. It should indicate version 1.2.

If you had to change your document root setting for this procedure, you may want to return the path to its original setting.

Go to “Upgrading the Software Utilities,” page 7 to complete the upgrade process.

Macintosh Platforms

To upgrade the Micro Webserver firmware using a Macintosh system, you must use the supplied Cisco Macintosh-specific cable and a terminal emulator program. For example, you can use the ZTERM application that is supplied with Global Village modems. If your Macintosh system does not have a terminal emulator program, you can use FreeTerm, or other terminal emulator shareware that is available on the Bulletin Board System (BBS) or the Internet.

Note The firmware upgrade process can take from 15 to 90 minutes, depending on the baud rate your Macintosh system can support. Quit all other applications before starting this procedure. After the upgrade is complete, ZTERM or your Macintosh system may be suspended. If so, restart your program or system.

To upgrade your Micro Webserver firmware:

Step 1 Unzip the mweb_fware12.ZIP file to a temporary directory on your local hard drive. For example, unzip the file contents to c:/upgrade/fware.

After the file is unzipped, you will see the Mw_r1024.hex file.

Step 2 Using the supplied Cisco Macintosh-specific serial cable, connect the serial port on the rear panel of the Micro Webserver to either the modem or printer port on your Macintosh system.

Step 3 Open your terminal emulator application and change the port setting to the serial port you used in Step 2.

For example, with ZTERM, open the program holding down the SHIFT key. Select either the modem or printer port. Or, use the serial port option within the **Settings: Modem Preference** menu item to set the serial port.

Step 4 Log in to the Micro Webserver as “root.”

Step 5 Set the download baud rate on the Micro Webserver. Through your terminal emulator program, enter *one* of the following console commands.

- For 9600 baud, enter:

  `diag load 9`

- For 57600 baud, enter:

  `diag load 5`

- For 19200 baud, enter:

  `diag load 1`

On the back panel of the Micro Webserver, the amber LED will flash and then stop as the baud rate is set.

Step 6 Set your terminal emulator baud rate to match the Micro Webserver baud rate. For example, with ZTERM, use the **Settings: Connection** menu item to set the baud rate.

Step 7 Set your terminal emulator delay parameters to zero for best performance (if these parameters exist in your program).

For example, with ZTERM, use the **Settings:Text Pacing** menu item to set all delays to zero.

Step 8 In your terminal emulator program, use the command for “send text file” to send the Mw_r1024.hex file to the Micro Webserver.

For example, with ZTERM, use the **File: Send Text** menu item.

Note Send the file as ASCII text. Do *not* use Zmodem, Xmodem, Kermit, or other options.

The upgrade process can take from 15 to 90 minutes, depending on the baud rate you select. As the upgrade progresses, your terminal emulator window should look similar to:

```
8000....9000...A000....B000....C000...D000...E000...F000
```

The Micro Webserver writes to flash ROM after the entire image is downloaded. You will see messages similar to:

```
...programming segment...
```

The Micro Webserver will reboot with the new firmware when the upgrade is completed.

Note Continue to wait until the Micro Webserver reboots. During this interval, the server is updating its Flash memory. While rebooting, the LED on the front of the Micro Webserver flashes red and green, and the 100% indication in the percentage bar flashes. Do *not* power off the Micro Webserver at this time. When the reboot is complete, the LED provide a blinking green indication and the 100% indication in the percentage bar stops flashing.

Step 9 To verify the firmware upgrade, Telnet to your Micro Webserver and check the login banner. It should indicate version 1.2.

Upgrading the Software Utilities

This section describes how to upgrade your BOOTP Server, Form Builder, and File Transfer Utilities version 1.1.

Note These software utilities are supported only on Windows 95 and Windows NT 4.x platforms.

To upgrade the software utilities on your PC:

Step 1 Make sure you do not have an earlier version of the utilities running.

Step 2 Uninstall the existing utilities:

Note Any profiles in your File Transfer Utility will be deleted.

(a) From your Windows Start menu, select Settings: Control Panel.

(b) Double-click the **Add/Remove Programs** icon.

(c) Select Cisco Micro Webserver DeInstaller in the list of programs.

(d) Click the **Add/Remove** button. You will be prompted to confirm this action. Click **Yes**. You will prompted to confirm deletion of shared files. Click **Yes to All**. You will be prompted to confirm this action. Click **Yes**.

Step 3 Unzip the mweb_util11.ZIP file to a temporary directory on your local hard drive, for example c:/upgrade/util.

Note For Windows platforms, Cisco recommends the use of WinZip to unzip the Cisco compressed files.

After the file is unzipped, you will see these directories: /disk1 and /disk2.

Step 4 Double-click the setup.exe file located in /disk1 to start the Cisco Micro Webserver Setup program. Follow the setup program prompts to complete the upgrade.

Step 5 Verify that you have installed version 1.1 of each utility:

(a) Open the File Transfer Utility and verify that the title bar indicates version 1.1.

(b) Open the BOOTP Server application and verify that the title bar indicates version 1.1.

(c) Open Form Builder and click the **?** icon on the toolbar. The **About** dialog box should indicate version 1.1.

Access Control List Mechanism

With Micro Webserver version 1.1 and later, it has been possible to create a new user and place access control on that directory in a single step. The behavior of this feature changed from version 1.0.

In version 1.0, access control on a user’s home directory was applied directly to the user name. This mechanism differed from the way access was applied for other directories, thus causing access control conflicts when two users had the same home directory.

With version 1.1 and later, access control on a user’s home directory is applied by creating a group, inserting the user into the group, and applying access to the group. All users with the same home directory are collected into the same group so that their access is applied as a single unit. The new group is named *aclgrp_N*, where *N* is a number (for example, aclgrp_9). Groups created in this way are automatically deleted when they are no longer referenced by the access control list system. No special user action is required.

With an upgrade from version 1.0, existing *home* directory protections are *not* automatically deleted or converted to the new scheme. Existing protections will continue to function exactly as before. However, newly created users will employ the newer protection scheme. If you want to ensure that only the new technique is used, delete the existing user access control information after upgrading from Version 1.0, and re-create user access setup using the new method.

Graphical User Interface Changes

With version 1.1 and later, the following button label changes have been made to the Users and Groups tabs (located under the Access tab in the configuration utility):

- **Users** tab

  The button which was labeled **Add** in version 1.0 is now labeled **Add/Modify**.

- **Groups** tab

  The button which was labeled **Add Users** in version 1.0 is now labeled **Add**.

Important Notes

The following notes provide helpful information on general product usage.

CD-ROM Support

When a SCSI CD-ROM drive is attached to the Micro Webserver, CD-ROM discs can be exported to the World Wide Web. The Micro Webserver is capable of reading CD-ROM discs in ISO9660 format, with or without Rock Ridge extensions. Rarely, a disc for Macintosh or UNIX systems uses another format. These discs cannot be read by the Micro Webserver.

SCSI Termination

Ensure that the SCSI termination switch on the back of the Micro Webserver is in the correct position: DOWN means SOME external devices. UP means NO external devices. If this switch is in the wrong position, the SCSI chain may still appear to work, but fail under high load. High-quality, 25 twisted-pair SCSI cables will also prevent disk failures in the future.

The system event log indicates the state of the SCSI switch at power up. Access http://<*webserver hostname*>/status/log.txt after power up to view this information. Beta-test Micro Webserver units have an earlier hardware release that incorrectly reports this information.

Root Password Recovery Utility

If you forget your root password and are running the Micro Webserver with a Windows platform, Cisco offers a program that allows you to reset your root password and access the server. Contact your customer service representative for details.

Micro Webserver Ambient Temperature

The Micro Webserver is rated for an ambient temperature of 20 to 32 degrees centigrade, due to the operational temperature of the ZIP media.

Data Backup

Cisco recommends that you always keep a backup of the software content on the ZIP media for your Micro Webserver in order to prevent the loss of data. You copy files using the Micro Webserver File Transfer Utility or your client FTP program.

ZIP Media Format

Cisco recommends that factory-fresh Iomega ZIP media and hard disks be formatted on the Micro Webserver before they are used, even if they are already formatted for use with DOS systems. The reformatting will significantly improve performance. Micro Webserver formatted disks are still read/writable by DOS and Windows systems.

PC Null Modem Cable

The null modem cable supplied for a PC has a “D” to “D” connection.

Macintosh System Serial Cable

The serial cable supplied for a Macintosh system has a “D” to “DIN” connection.

Write-protected Disks

The Micro Webserver will not write on write-protected ZIP media, such as the ZIP TOOLS disk that comes with external IOMEGA drives. Attempts to write to or format these disks fail with error 51. There is no way to set or remove the “write protected” attribute of ZIP disks using the Micro Webserver.

Disk File (DF) Console Command

You can use the disk file (DF) command to determine the amount of free space on your Micro Webserver ZIP drive. Telnet to the Micro Webserver and enter the following command at the console:

df /1

A sample output follows:

```
f_type        0
f-flags       4096
f_bsize       8192L
f_iosize      8192L
f_blocks      12280L
f_bfree       4965l
f_bavail      4965L
f_files       512L
f_fmetaerrs   OL
f_fdirerrs    OL
f_fsid        305724218L
```

To determine the amount of Micro Webserver ZIP disk space that is being used:

1. Determine the file systems size by multiplying the values of *f_blocks* by *f_bsize*. In this example, the result is approximately 100 MB.
2. Determine the free space multiplying the values of *f_bavail* by *f_bsize*. In this example, the result is approximately 40 MB.
3. Determine the amount of file space that is being used by subtracting the free space from the file systems size. In this example, the result is approximately 60 MB.

When using the DF command, keep in mind:

- In rare cases, due to power failures, abrupt power interruption, SCSI cabling faults, or disk hardware problems, the file system image can become corrupted. The Micro Webserver detects, but does not fix disk corruption. The Micro Webserver disk file (**DF)** console command lists two counters, indicating the number of file system corruption errors encountered since the disk was initialized. (To access console commands, Telnet to the Micro Webserver.) These counters should normally be zero. If they are non-zero, then the disks are corrupted. It is best to handle corruption before potentially valuable data is lost.
- The Micro Webserver does not have a built-in program such as SCANDISK or CHKDSK. To fix a disk that is corrupted, back up the disk to another device (for example, a PC file system). Then reformat the disk and recopy the data to the disk. If you have a ZIP drive on your PC, you can use SCANDISK to repair Micro Webserver ZIP media.
- A directory must be empty before it can be removed. If a disk image is corrupted, a directory can appear to be empty, but actually contain corrupted entries. In this case, the directory delete command will fail with a “directory not empty” error.

FS: H bit, S bit, R bit

The Micro Webserver ignores the MS-DOS file system “H” (hidden) and “S” (system) bits. Hidden and system files appear as normal files, and may be deleted or overwritten, as permitted by other system protections. The Micro Webserver has some treatment of the “R” (read-only) bit. If the R bit is set on a directory, then files may not be deleted from this directory. Super-users can delete files from these directories. There is no way to set or reset the H, S, or R bits using the Micro Webserver. The only way to have a directory or file with one or more of these bits set is to place the ZIP media in a PC ZIP drive.

Using a Macintosh System to Set the Micro Webserver IP Address

To set the Micro Webserver IP address using a Macintosh system, you must use the supplied Cisco Macintosh-specific serial cable and a terminal emulator program. For example, you can use the ZTERM application that is supplied with Global Village modems. If your Macintosh system does not have a terminal emulator program, you can use FreeTerm, or other terminal emulator shareware that is available on the Bulletin Board System (BBS) or the Internet.

To set the Micro Webserver IP address:

Step 1 Using the supplied Cisco Macintosh-specific serial cable, connect the serial port on the rear panel of the Micro Webserver to either the modem or printer port on your Macintosh system.

Step 2 Open your terminal emulator application and change the port setting to the serial port you used in Step 1.

For example, with ZTERM, open the program holding down the SHIFT key. Select either the modem or printer port. Or, use the serial port option within the **Settings: Modem Preference** menu item to set the serial port.

Step 3 In your terminal emulator program, set the communications parameters to: 9600 baud; no parity; 8 bits; and 1 stop bit (9600, N, 8, 1) with no flow control.

Step 4 Log in to your Micro Webserver as "root."

Step 5 Set the Micro Webserver IP address. Through your terminal emulator program, enter the console command:

```
config nvram internet-address xxx.xxx.xxx.xxx
```

where *xxx.xxx.xxx.xxx* is the IP address.

Step 6 Write the IP address to memory and reboot the Micro Webserver. Through your terminal emulator program, enter the console commands:

```
config nvram write
reboot
```

Converting Form Builder File Formats to Extract Data

Form Builder is a tool for creating standalone HyperText Markup Language (HTML) forms or for adding forms support to existing HTML documents. You must be running on a Windows 95 or Windows NT 4.x platform to use the Form Builder Version 1.0 application.

fdbcsv.exe is the utility used to convert a file from the Form Builder application .fdb format to .csv format and vice versa. In .csv format, you can use Microsoft Excel, Microsoft Access, or another program that supports comma-separated variables to compile and analyze the data gathered through HTML forms.

The fdbcsv.exe utility is installed in c:\program files\cisco\micro webserver. The command syntax is:

fdbcsv [*-v*] *infile outfile*

The *-v* option displays all records generated.

The *infile* option indicates the .fdb file or .csv file.

The *outfile* option indicates the .fdb file or .csv file.

For example, to convert the file data.fdb to .csv format, you would:

Step 1 Use FTP or the Micro Webserver File Transfer Utility to transfer the data.fdb file from the Micro Webserver to your Windows system.

Step 2 Convert the data.fdb file to data.csv format:

```
c:\>fdbcsv data.fdb data.csv
```

Note To convert data.csv back to data.fdb (.fdb format), use the command:

```
c:\>fdbcsv data.csv data.fdb
```

Syslog Files

The Micro Webserver can log router Syslog files and track system errors, reboots, and other key maintenance information. The syslog.log file will automatically be generated in the Micro Webserver /zip-100/etc/log directory.

There can be only one log file on a Micro Webserver at any time. Set up your network so that only *one* router sends syslog files to any *one* Micro Webserver. The default size for the Micro Webserver syslog.log file is 8 KB. The maximum file size is 1258291 bytes. (The file size is limited to the maximum 1.2 GB external SCSI hard disk you can attach to the Micro Webserver.)

To search for a specific pattern on syslog.log or the customized name of your Syslog file, use the Search application on the default Micro Webserver home page. Enter any pattern for the file in the /zip-100/etc/log directory.

The following example illustrates how to send Syslog messages from your router to the Micro Webserver. In this example, the router name is *eng-router.* The Micro Webserver name is *cisco-microweb.* The logging notification level is set to *warnings*.

At the router prompt, enter the following commands:

```
eng-router#conf t
eng-router(config)#logging cisco-microweb
eng-router(config)#logging trap warnings
eng-router(config)#end
```

Logging notification levels are listed in Table 2.

Table 2 Logging Notification Levels

Level	Description
emergencies	System is unusable
alerts	Immediate action needed
critical	Critical conditions
errors	Error conditions
warnings	Warning conditions
notifications	Normal but significant conditions
informational	Informational messages
debugging	Debugging messages

Cisco recommends that you use the debugging level *only* for Cisco 750 series, Cisco 1000 series, Cisco 2500 series, and Cisco 4000 series routers. Debugging messages generate large files and create a heavy traffic load for the Micro Webserver. All other levels of Syslog can be performed for all Cisco routers, including the Cisco 7000.

For the latest updates on Syslog recommendations, visit Cisco at http://www.cisco.com.

Remote Copy Protocol Commands

Remote copy protocol (rcp) is set up to automatically work with “root” on a UNIX host. To use rcp with a router, create a user with the same name as the host name of the router and place the user in the group “rcp.”

Step 1 Open the configure application. Select the **Users** tab under the **Access Control** tab.

Step 2 Create a user with the *same name* as the host name of the *router*.

> **Note** All routers which need to use rcp with the Micro Webserver *must* have a corresponding host name in the group “rcp.”

Step 3 Leave the Password and Confirm fields blank.

Step 4 In the Home field, enter the directory where you want the **rcp** command to copy to and from the Micro Webserver. Cisco recommends you create an rcp directory and create a subdirectory, using the router host name, for each router within the rcp directory.

Step 5 Set the read and write permissions.

Step 6 Click **Add/Modify**.

Step 7 Select the **Groups** tab under the **Access Control** tab.

Step 8 Highlight the “rcp” group under the Group list and select the user you just created for the router. Click **Add** to add the user to the “rcp” group.

rcp commands on the router include:

- **write net**
- **copy flash rcp**
- **copy rcp flash** (if you have an image under the router's home)
- **copy startup-config rcp**
- **copy rcp running-config** (if you have a configuration file in /zip-100/etc/tftpboot)
- **copy running-config rcp**

The following is an example of an **rcp write** command. In this example, the name of the Micro Webserver is *cisco-microweb*. The router name is *cisco-router*.

```
cisco-router#copy flash rcp
PCMCIA flash directory:
File Length   Name/status
 1   1243747 master/c1000-ny-mz.111-6
[1243812 bytes used, 2950492 available, 4194304 total]
Address or name of remote host [cisco-microweb.cisco.com]?
Source file name? master/c1000-ny-mz.111-6
Destination file name [master/c1000-ny-mz.111-6]? zip-100/c1000
Verifying checksum for 'master/c1000-ny-mz.111-6' (file # 1)... OK
Copy 'master/c1000-ny-mz.111-6' from Flash to server
 as 'c1000'? [yes/no]yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash copy took 00:00:28 [hh:mm:ss]
cisco-router#
```

The Micro Webserver-based rcp server has several differences from a UNIX-style rcp server:

- The /etc/hosts.equiv file is replaced by the rcp group. To access the Micro Webserver using rcp, the user must have (1) a valid user name on the Micro Webserver, (2) a user name and IP source address that matches the rcp group, and (3) permission to access the directory involved.
- The **rcp** *-p* option is not supported.
- The **rcp** *-r* option has an internal limit to the depth of directory that it can transfer to the remote host. If the directory is more than 19 levels deep, rcp will not descend further into the directory structure, and an error results.
- The **rcp** *-r* option is also adjusted so that the destination directory must be specified. That is:

  ```
  rcp -r mydir microweb:/zip-100/mydir
  ```

  will create the directory /zip-100/mydir.

  In the following example, if you are logged in to the UNIX host cisco-unix as the user “rcpuser,”

  ```
  cisco-unix%rcp -r mydir cisco-microweb:
  ```

  will transfer the directory “mydir” and all of its contents to the home directory of “rcpuser” on the Micro Webserver. If the home directory of “rcpuser” on the Micro Webserver is /zip-100/home/rcpuser, the new directory will be called /zip-100/home/rcpuser/mydir.

TFTP Commands

The default paths of the TFTP directories and Syslog files are different. It is important that the TFTP Read Directory and TFTP Write Directory are different directories. Typically, the Write Directory is a subdirectory of the Read Directory. This is a security issue, so that TFTP clients which are allowed to write into the TFTP Write Directory are not permitted to modify the files (typically router images) in the TFTP Read Directory.

For TFTP commands, the following directories on the Micro Webserver are used:

- TFTP reads:

  /zip-100/etc/tftpboot
- TFTP writes:

  /zip-100/etc/tftpboot/tftp_put

TFTP write commands are router commands, such as:

- **write net**
- **copy flash tftp**

  This command will, by default, upload from Flash memory on the router to the /zip-100/etc/tftpboot/tftp_put directory on the Micro Webserver.
- **copy tftp flash**

  This command will, by default, get the specified file from the Micro Webserver's /zip-100/etc/tftpboot directory and download the file to the router.
- **copy startup-config tftp**
- **copy tftp running-config** (if you have a configuration file in /zip-100/etc/tftpboot)
- **copy running-config tftp**

The following is one example of a **tftp** write command. In this example, the Cisco Micro Webserver name is *cisco-microweb.* The router name is *ij-router.*

```
ij-router#copy flash tftp
System flash directory:
File Length   Name/status
 1   4050356 master/igs-c-l.111-7.3
[4050420 bytes used, 4338188 available, 8388608 total]
Address or name of remote host [255.255.255.255]? cisco-microweb
Translating "cisco-microweb"...domain server (171.69.2.132) [OK]
Source file name? master/igs-c-l.111-7.3
Destination file name [master/igs-c-l.111-7.3]? igs-c-l.111-7.3
Verifying checksum for 'master/igs-c-l.111-7.3' (file # 1)... OK
Copy 'master/igs-c-l.111-7.3' from Flash to server
 as 'igs-c-l.111-7.3'? [yes/no]yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash copy took 00:01:32 [hh:mm:ss]
ij-router#
```

Note Make sure that there is *no* directory specified. The destination filename can only be a file. The Micro Webserver TFTP process will not write outside of its TFTP write directory.

The flash will be saved in the volume /etc/tftpboot/tftp_put/igs-c-l.111-7.3.

The destination supports long filenames. You do not have to create the path. All TFTP puts will be in the volume /etc/tftpboot/tftp_put directory.

General Caveats

This section describes possibly unexpected behavior by Micro Webserver version 1.2.

Access Control User Deletion and Save Button [CSCdj08774]

If you delete a User from a Group in the Groups tab under the **Access Control** tab, the **Save** button will not flash. In order to save this deletion, you must remember to click the **Save** button before you reboot or your user deletion will not occur.

Access Control User "Everyone" Deletion from rcp Group [CSCdj08806]

You cannot delete the user "Everyone" from the "rcp" group. If you want to remove "Everyone" from the "rcp" group, you must Telnet to the Micro Webserver and enter one the following commands at the console.

If your "rcp" group has the user "Everyone" and other users in it, enter:

```
config group del rcp Everyone
```

If your "rcp" group has *only* the user "Everyone" in it, enter:

```
config group del rcp
```

Access Control Permissions [CSCdi83341]

If a user is created in the **Users** tab and the Permit Others option is *not* allowed for either read or write, the Micro Webserver applies these changes to the access control list (ACL), but changes are not reflected correctly in the graphical user interface (GUI). After a user clicks the **Apply** and **Save** buttons, the Permit Others field indicates that the Read permission is checked, or allowed. The access control list functions correctly, however.

Firmware Upgrade for Macintosh Users [CSCdi83042]

If you are using a Macintosh system with the Micro Webserver, you cannot use the **Upgrade** tab in the **configure** application to upgrade your Micro Webserver firmware. You must use the procedure listed under "Macintosh Platforms," page 5.

File Browser Dialog Box

The following caveats apply to the file browser dialog box:

- If you are using Netscape 3.01 or later on a SunOS 4.1.3 platform, the file browser dialog may not function properly. [CSCdi82820]
- Because the file browser dialog box scroll bars do not function properly under Netscape 3.0 for Windows 95, you must click the arrows to move up and down in the window. [CSCdi83047]

Micro Webserver Applications Are Not in Compressed CAB Format [CSCdi83070]

Micro Webserver applications are not in compressed CAB format and do not support faster downloads on MSIE.

Form Builder Application (formbuilder.exe)

The following caveats apply to the Form Builder application:

- You cannot set a radio button as the default choice. [CSCdi82768]
- Double clicking the xxx.swz file launches the Form Builder application, but may not open the xxx.swz file. [CSCdi83069]

File Transfer Utility (mwftu.exe)

The following caveats apply to the File Transfer Utility:

- On connecting to an invalid IP address, the application provides the login screen without reporting any errors. [CSCdi82762]
- The scroll bar response is slow. [CSCdi82784]
- Wildcard characters (*) do not work when you click the Refresh button. You need to press the Enter key. [CSCdi82793]

BOOTP Server Application (bootp.exe)

The following caveats apply to using the BOOTP Server application:

- The Micro Webserver name is not configured. [CSCdi82816]

  A node name is optional and only for reference when using BOOTP Server program. It is not passed to the Micro Webserver.
- The BOOTP Server does not assign a subnet mask or default gateway IP address. [CSCdi82819]

  Use the **General** tab in the **configure** application to set these parameters.

Version 1.1 Caveats/Version 1.2 Modifications

The following caveats apply to version 1.1 but were fixed in version 1.2.

Telnet Server

Fixed Telnet initialization so FTP is not disabled when Telnet is turned off. Previously if Telnet was disabled and the Micro Webserver system were rebooted, FTP was not properly initialized.

FTP Server

Fixed FTP server so that underlying **delete**, **mkdir**, **rmdir**, and **rename** functions check access control list credentials. This general security fix routes FTP commands through a check of access control list credentials so that a properly administered Micro Webserver has protection for files on the server.

Console (CLI)

The following changes apply to the Micro Webserver's console or command line interface (CLI):

- Restricted permissions on the commands **newfs** and **init-ram**. User must now be root (or equivalent of) to get access to these commands.
- Fixed access control list credential checking in the command line interpreter. The underlying code for the commands **type** (equivalent of **more**), **rm** (equivalent of **unlink**), **mv**, **md**, and **rd** are routed through a check of access control list credentials. This fixes access control list credential checking for console users, Telnet guests, HTTP guests, and for rcp commands used with the Micro Webserver.

HTTP Server

The following changes apply to the Cisco Micro Webserver HTTP server:

- Fixed an initialization error in HTTP socket read. This bug caused corrupted posts.
- Fixed a memory leak in posting of files. The HTTP server would not free the memory it was allocating for each post. After many posts, the system would run out of memory causing various out-of-memory errors, including truncated posts. This fix prevents this memory leaks from occurring.
- Fixed a bug that occurred while deleting MIME type entries from the MIME tab form in the **Maps** tab in the **configure** application. This bug occurred when deleting the second entry in the MIME type and comment fields. The first entry would get deleted instead. The fix allows correct deletion of MIME type and comment fields.

File System

Directory entries for files in subdirectories that have more than 256 files had the potential of being corrupted on the previous release of the firmware. File system corruption occurred when a non-root directory grew beyond the size of a cluster. This was more evident on an IOMEGA-formatted zip disk because the default cluster size is 2K. A newly formatted file system which defaults to 8k clusters showed the symptoms when a non-root directory exceeded 256 files (or less if the file names were long). The directory entries beyond the 256th directory entry would become corrupted by an improper update. A file system code change fixes this problem and allows directories to grow to multiple clusters without corruption occurring. File systems that had this corruption problem should be backed up, and then checked through the **scandisk** command, or they should be reformatted.

Time Functions

In version 1.1, there was a bug in the handling of +year 2000 dates in Netscape 3.0 and 3.1. Specifically, Netscape would crash if it tried to access an item in its cache that has a reported modification date of later than 2037. (This is the date when UNIX time values go "negative.") These values were translated to dates later than the year 2037. This has been fixed. Symptoms of the Netscape crash included repetitive crashes because of cached pages that contained the bad date information. To clear bad pages from Netscape's page cache, go to the Netscape Options menu and select Network preferences. In the Cache tab, clear Netscape's memory and disk cache.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

This document is to be used in conjunction with the *Cisco Micro Webserver Quick Reference Guide* and *Using Cisco Micro Webserver* publications.